EPAS: Efficient Privacy-preserving Authentication Scheme for VANETs-based Emergency Communication

Xuedan Jia[1]
[1]School of Computer Science and Telecommunication Engineering, Jiangsu University, Zhenjiang, China
Email: laura_j@163.com

Xiaopeng Yuan[2], Lixia Meng[3], Liangmin Wang[1, 3]
[2]School of Electronic Engineering and Optoelectronic Techniques, NUST, Nanjing, China
[3]Key Laboratory of Intelligent Computing & Signal Processing, MOE, Anhui University, Hefei, China
Email: (wanglm@ujs.edu.cn)

***Abstract*—Vehicular Ad Hoc Networks (VANETs) can provide participants with security services and entertainment information during the driving. To guarantee correct and smooth operations of VANETs, it is necessary to achieve efficient authentication with user privacy preserving. Current solutions either cannot satisfy privacy requirements, or are not efficient in message verification. Moreover, all the existing schemes are RSU-based. We, for the first time, apply VANETs to emergency communication during disaster rescue, and effective authentication scheme is proposed in accordance with the actual environment, where there is no fixed road-side unit (RSU). In this paper, we present an efficient identity based signature scheme EPAS, which satisfies conditional privacy requirements through software solution. In aspect of efficiency, both lightweight signature and batch verification are employed to provide effective authentication. Extensive theoretical and experimental analyses demonstrate the security and efficiency of EPAS in terms of privacy-preserving and low authentication delay.**

***Index Terms*—Vehicular Ad Hoc Networks; Emergency Communication; Conditional Privacy Preserving; Batch Verification**

I. Introduction

Vehicular ad hoc networks (VANETs) are a kind of specific wireless sensor networks of vehicles, equipped with wireless communication devices. The vehicles can communicate with each other (V2V) and with the road-side units RSUs (V2R) by means of the Dedicated Short-Range Communication protocol (DSRC) [1] providing drivers with traffic information for driving safety [2], and infotainment information to improve the driving experience [3]. According to DSRC, vehicles broadcast traffic safety message every 100-300ms. In high traffic density scenario, verifying every message will bring great computation overhead. In addition to computational efficiency, privacy requirements are also essential as the safety packet contains privacy-related information about user's geographical location and personal predilection. To make VANETs practical in use, security and privacy requirements must be guaranteed first of all other issues. Lots of schemes [4-15] have been devoted to solve the above problems with [4][5][10-13] dedicated to driving safety assurance, and [14] for entertainment services, respectively. But all these schemes are based on the assumption that RSUs cover the entire network, which is unrealistic during the initial deployment of VANETs and inapplicable to emergency communication in disaster conditions.

Recently, large-scale natural disasters have occurred frequently over the world. Taking Wenchuan earthquake [16] as an example, the disaster-affected area was an isolated island to some extent as infrastructures including communication, transportation, and power facilities were destroyed. Wireless emergency communication system is imperative to collect real-time information and give feedbacks. There have been researches dedicated to routing [17] in ad hoc networks, and vehicle routing [18][19], but no emergency communication scheme based on VANETs has been proposed.

We, for the first time, apply VANETs to emergency communication during disaster rescue. A specific network model is proposed, as shown in Fig. 1. During

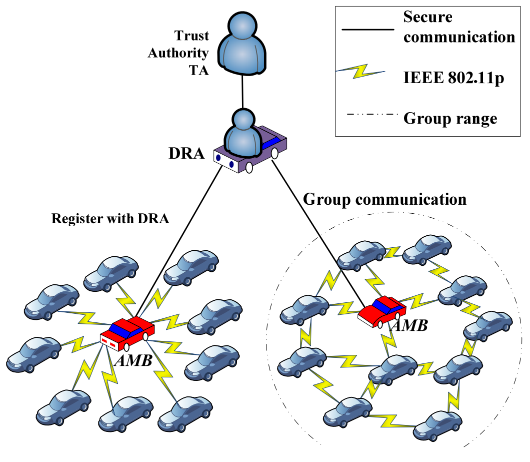


Figure 1. Network model

doi:10.4304/jsw.8.8.1914-1922

emergency communication, no fixed infrastructure existing, vehicles in the disaster area need to register timely with the authority for subsequent communication. Therefore, secure and efficient scheme is needed for vehicle registration and communication in the absence of fixed RSU. In addition, privacy requirements and authentication efficiency should be guaranteed. Thus, an Efficient Privacy-preserving Authentication Scheme (EPAS) is proposed based on the network model. We assume the disaster relief authority (DRA) and emergency communication cars (ambulances or fire trucks, *AMBs* for short) enter the disaster-affected area. Vehicles in the area can register themselves with DRA via *AMB* for subsequent rescue communication.

II. Related Works

Researches in secure authentication and privacy protection have been quite active in recent years. Numbers of schemes have been proposed. According to the pattern in which messages are verified, these existing authentication schemes can be classified into two categories, i.e., one-by-one message verification [9]-[12] and batch verification [13]-[15] schemes. In addition, there are many schemes dedicated to privacy problem [4]-[8].

For privacy protection in VANETs, there are two kinds of commonly used technique, group signature and Mix-zone pseudonym-changing pseudonym within specified region. TACK [4] and TARI [5] both adopted [6], a group signature mechanism which supported tracking and revocation of anonymous signature, to obtain short-term anonymous certificates. For existence of group managers, a ring signature scheme [7] was proposed to meet privacy protection without group manager. Reference [8] aimed to establish Mix-zones at social points to achieve privacy protection. However, Mix-zone pseudonym scheme is vulnerable to terrain-based monitoring technologies, while both group signature and ring signature are time consuming in verification.

The one-by-one verification schemes are characterized by simple to use and large verification delay. In 2007, Raya, etc. proposed [9] to realize authenticity and privacy. However, public key infrastructure (PKI) based scheme has the problem of certificates transmission and management. Subsequently, Lin et al. proposed a group signature scheme GSIS [10], eliminating the public key certificates. RAISE [11] was a RSU-assisted verification scheme. Secret key shared between vehicle and RSU was used to generate message authentication code (MAC). Nevertheless, RSU authenticated message one by one and broadcasted 128B hash value for each valid message, which brought heavy communication burden. CMAP [12] embraced cooperation verification idea to improve efficiency. Verifiers were chosen based on location, and non-verifiers waited for the verifier's results. Due to the uncertainty of the vehicle speed and road conditions, the scalability and practicality of CMAP are facing questioning.

All the above schemes are not efficient as the number of messages can be very large in VANETs. IBV [13] devised identity based (ID-based) signature to realize batch verification. IBV's major flaw is that any malicious vehicle V_j can easily forge the signature of V_i. In addition, it can't detect invalid signatures. If the verification fails, all messages will be discarded. ABAKA [14] was merely devised to entertainment service. CPAS [15], adopted pseudonyms to protect privacy and realize batch verification between the vehicle and the RSU. But the Private Key Generator (PKG) is essential to generate user private key, i.e. key escrow. In addition, signature verification is based on bilinear pairing operation which is of large computational overhead.

The comparison of the aforementioned programs is shown as Table Ⅰ, from which we can see they are all not applicable to emergency communication, as roadside infrastructures are assumed to cover the entire network in all the schemes. To apply VANETs to emergency communication, we present an Efficient Privacy-preserving Authentication Scheme (EPAS) in this paper. In allusion to the conditional privacy problem, an exclusive secret key is established between the vehicle and DRA, only allowing DRA to track malicious vehicles from the pseudonyms. In addition, lightweight signature and batch verification are combined to reduce computation and communication cost, providing fast and efficient authentication. In addition, for vehicle group communication, a group formation scheme is presented to allow vehicles to efficiently authenticate each other in the same group.

TABLE I.
COMPARISON OF RELATED WORKS

Schemes	Communication patterns	Cryptographic basis	Conditional privacy preserving	Batch verification	Emergency communication	
					No RSU	Vehicle group communication
TACK[4]	V2R	Group Signature	√	×	×	×
GSIS[10]	V2V & V2R	Group & ID-based Signature	√	×	×	×
RAISE[11]	RSU-based V2V	PKI Signature & MAC Code	√	×	×	×
CMAP[12]	V2V	Group Signature	√	×	×	×
IBV[13]	V2R	ID-based Signature	×	√	×	×
CPAS[15]	V2R	ID-based Signature with PKG	√	√	×	×

III. System Model And Preliminaries

VANETs for emergency rescue are different from the ordinary network model, as the RSUs are seriously damaged. We propose an appropriate network model and an efficient authentication scheme suitable for this model. To facilitate the specification of our scheme, we first briefly describe the system model, the design objectives and the basic presuppositions.

A. System Model

The actual circumstance we consider is emergency communication in disasters relief. According to the accurate environment, a two-layer network model is proposed, as shown in Fig. 1. The upper layer comprises the Trust Authority (TA) and the disaster relief authority DRA, while the lower layer is composed of vehicles and *AMBs*. TA is responsible for issuing real identification *RID* to vehicles and private/public key pairs to all parties. Most importantly, TA is always trusted and can never be compromised. So is DRA, who has made contract and can communicate securely with TA.

AMBs are equipped with powerful devices of stronger computation and communication capability than regular vehicles. The communication range of *AMB* can be larger than that of ordinary vehicles. Within its communication range, *AMB* is responsible for forwarding in-time registration messages from vehicles to the DRA and assisting group formation. *AMBs* communicate securely with DRA. In Fig. 1, the dotted line indicates the communication range of a group, in which vehicles communicate with each other based on the wireless communication standard IEEE 802.11p. There are two types of communication in our model: the vehicle to DRA communication (V2D) and the vehicle group communication (V2V). DRA verifies vehicle messages in batch to save the computational overhead, and takes comprehensive data analysis for reasonable rescue plans.

B. Design Objectives

In vehicular ad hoc networks for emergency communication, an efficient authentication scheme needs to satisfy the following six goals: registration without RSU, sender authentication and message integrity, conditional privacy, revocability, low communication overhead and fast verification, and internal attacks prevention, which are further discussed as below.

Registration without RSU: There is no RSU in the emergency communication. Efficient vehicle registration scheme is needed for vehicles without RSUs, as they can authenticate each other only after registration.

Sender authentication and message integrity: The receivers need to authenticate that the messages are indeed sent by legitimate entities and are not tampered during the transmission. This is enforced by signatures.

Conditional privacy: A secure scheme must prevent eavesdroppers from getting the private key of vehicles or linking to the vehicle's real identity from the messages. On the other hand, when the malicious vehicles are found or vehicles are in dispute for an emergency accident, it's necessary to allow the TA to trace back to the vehicle's real identity.

Revocability: When vehicles are in dispute or the content of a message is bogus, the authority should be able to retrieve the real identity and revoke it from the network. The authority notifies the network of illegal vehicles in time, preventing the revoked vehicle from participating in the communications.

Low communication overhead and fast verification: Due to the urgent time requirement of message authentication and limited bandwidth, safety verification program should also consider the efficiency requirements in terms of low communication overhead and fast authentication.

Internal attacks prevention: Legitimate vehicles cannot get the key information of other vehicle, or forge a legal signature of the other vehicle. Even if some vehicles are captured by the attacker, the attacker can't obtain other legitimate vehicle's private key with the captured vehicles.

C. Basic Presuppositions

An elliptic curve is a cubic equation of the form $y^2+axy+by=x^3+cx^2+dx+e$, where a, b, c, d, and e are all real numbers. In an elliptic curve cryptography (ECC) system, the elliptic curve equation is defined as the form of $\mathrm{E}q(a, b)$: $y^2=x^3+ax+b$ (mod q), over a prime finite field F_q, where $a, b\in \mathrm{F}_q$, $q>3$, and $4a^3+27b^2\neq 0$(mod q) [20]. In general, the security of ECC depends on the difficulties of the following problems [21][22].

Definition 1. *Elliptic Curve Discrete Logarithm Problem (ECDLP)*

Given two points P and Q over $\mathrm{E}q(a, b)$, the elliptic curve discrete logarithm problem (ECDLP) finds an integer $x\in \mathrm{F}_q$ such that $x\cdot P=Q$.

Definition 2. *Computational Diffie-Hellman Problem (CDHP)*

Given three points P, sP and tP over $\mathrm{E}q(a, b)$ for $s, t\in \mathrm{F}_q$, the computational Diffie-Hellman problem finds the point $(st)P$ over $\mathrm{E}q(a, b)$.

IV. Epas

The proposed Efficient Privacy-preserving Authentication Scheme (EPAS) employs identity based cryptography. Thus, there is no delivery and management of certificates. In consideration of computational overhead, point multiplications instead of bilinear operations are used to generate lightweight signature. Thus the computation overhead and communication overhead are largely saved. Specific to the privacy destruction problem caused by key preload, session key agreement protocol is proposed to establish an individual session key between vehicle and the credible authority DRA during vehicle registration. This sincerely guarantees the conditional privacy protection requirements. The Effective Privacy-preserving Authentication Scheme (EPAS) is composed of two sub-schemes: Scheme1 and Scheme2, for vehicle to DRA communication and vehicle group communication respectively. The prime symbols used in the paper are defined as the following Table Ⅱ.

TABLE II.
NOTATION

Notation	Description
TA	Trust Authority
DRA	Disaster Relief Authority
AMB	Emergency Communication Car
V_i	Vehicle
RID_i	Real Identity of Vehicle *i*
PK_{DRA} / SK_{DRA}	Public/Private Key of DRA
PK_i / SK_i	Public/Private Key of V_i
h	One-way Hash Function h:$\{0,1\}^*\rightarrow \mathbf{Z}_q^*$
H	Map to Point Function H: $\{0,1\}^*\rightarrow G$
k_i	Shared Secret between V_i and DRA
ID_i	Pseudonym of V_i
CSK_i	Corresponding Private Key of ID_i
GPK_i	Group Public Key of V_i
GSK	Group Secret Key
||	Concatenation Operation

A. System Initialization and Vehicle Registration

1. System initialization

According to the standard IEEE1609.2 [23], there exists PKI to provide key management. The DRA and vehicles have a pair of public/private keys and the public key certificate signed by TA. System initialization is completed by TA to establish the public parameters of the system.

- Let *G* be a cyclic additive group generated by the *P* with the order *q*;
- TA picks *h*, *H*, and establishes the public parameters $\{G, q, P, h, H\}$;
- DRA, *AMBs*, and vehicles download the system parameters $\{G, q, P, h, H\}$ from TA;
- The DRA randomly chooses $s \in \mathbf{Z}_q^*$ as its private secret key used to generate group secret key.

2. Vehicle registration

During the registration process, a session key agreement scheme is proposed to establish a shared secret between vehicle and DRA via *AMB*, as shown in Fig. 2. The secret is just known to the vehicle itself and the DRA, thus ensuring only the DRA can trace to the real identity of a vehicle, and revoke malicious vehicle from the network. This can be achieved by the modified Diffie-Hellman session key agreement scheme secured with signature. The processes of mutual authentication and key agreement are shown as follows.

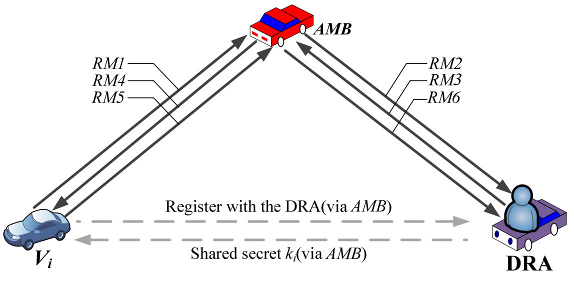


Figure 2. Vehicle registration

Step1: First, vehicle V_i randomly selects $a \in \mathbf{Z}_q^*$, and concatenates the random element P^a and its real identity. Next, V_i encrypts the concatenation with the DRA's public key. Then V_i encrypts the concatenation of the encryption and the time stamp and gets *RM1* as

$$RM1 = (\mathrm{T}_i \| (P^a \| RID_i)_{PK_{DRA}})_{PK_{AMB}} \tag{1}$$

Finally, V_i sends *RM1* to the *AMB*.

Step2: Receiving the first message *RM1* from vehicle V_i, *AMB* decrypts and verifies the time stamp. If the message is new, it delivers the rest part of the message, i.e., *RM2*, to DRA securely. Otherwise, it discards the message and waits for new registration messages.

$$RM2 = (P^a \| RID_i)_{PK_{DRA}} \tag{2}$$

Step3: DRA decrypts the message and verifies the real identity RID_i. If RID_i is in the revoke list (RL), the message is abandoned. Otherwise, DRA randomly chooses $b \in \mathbf{Z}_q^*$, gets k_i=P^{ab}. Next, DRA signs the concatenation of P^a and P^b and then encrypts the signature and P^b by V_i's public key. Then the encrypted message

$$RM3 = (P^b \| (P^a \| P^b)_{SK_{DRA}})_{PK_i} \tag{3}$$

is sent to *AMB* securely.

Step4: *AMB* passes the message to vehicle V_i.

$$RM4 = RM3 \tag{4}$$

Step5: The vehicle verifies the DRA's signature, and if valid, sends its own signature on P^a and P^b to the DRA via *AMB*.

$$RM5 = (P^a \| P^b)_{SK_i} \tag{5}$$

Step6: DRA authenticates the signature. If it's valid, a shared secret between V_i and DRA has been established through the above steps.

$$RM6 = RM5 \tag{6}$$

The shared secret is k_{i}=P^{ab}, which is employed to generate pseudonyms by the vehicle V_i. The actual identity of the vehicle can only be traced by DRA to ensure the conditional privacy protection.

B. Pseudonym Generation

In the identity based cryptography, the entity's public key can be generated based on its identity. Compared to traditional PKI based scheme, there is no certificates management and transportation. Thereby computation and communication overhead are greatly economized. Different pseudonyms are used to sign messages during the communication process, to protect the vehicle's location privacy from being tracked or associated.

The pseudonym ID_i consists of three parts: ID_i^1, ID_i^2, LT_i, where ID_i^1 and ID_i^2 are the pseudonym material and LT_i is the pre-defined life period of the pseudonym. First of all, the vehicle selects a random number $r_i \in \mathbf{Z}_q^*$ to establish point $R_i \in G$, so that R_i=(x_i, y_i)=r_iP. The vertical and horizontal coordinates of each point of are integers within F_q . Then, the vehicle generates pseudonym as $ID_i^1{=}h(R_i)$, $ID_i^2{=}RID_i \oplus H(k_i||ID_i^1 \,||\, LT_i)$, which only allows the DRA to reveal the real identity of malicious vehicles. Because only the vehicle and the DRA know the secret generating the pseudonym, the third party is unable to obtain the true identity of the vehicle. The corresponding private key CSK_i is $CSK_i{=}h(ID_i||k_i)P$. So the vehicle V_i generates its own pseudonym as

$$\begin{cases} ID_i = (ID_i^1, ID_i^2, LT_i) \\ ID_i^1{=}h(R_i) \\ ID_i^2{=}RID_i \oplus H(k_i||ID_i^1 \,||\, LT_i) \end{cases} \tag{7}$$

and the corresponding private key as

$$CSK_i{=}h(ID_i||k_i)P \tag{8}$$

In the end, the vehicle V_i stores a list of the pseudonyms ID_i with its corresponding private key CSK_i and the random points R_i.

Notice that, 1) it's essential to insert life period LT_i into every pseudonym to prevent attackers from abusing obsolete pseudonyms; 2) the pseudonyms and the private keys can be completed prior to joining the network communication. Thus, the delay of signing a message does not include the time generating a pseudonym and the private key.

C. EPAS

When facing a mass of VANETs messages, vehicles may be not able to verify every message before its deadline as the large computational overhead, resulting in high packet loss rate. While packet loss may seriously impact the security applications, saving computational overhead is a major consideration for vehicles' limited resources. Point multiplications are adopted instead of bilinear operations to sign and verify message, as one pairing operation costs 4.5ms while the point multiplication only 0.6ms [24]. In addition, batch verification allows verifier to authenticate messages in batch to provide high efficiency.

1. Scheme1:V2D communication

The vehicle V_i's signature σ_i on message M_i consists of two parts, $\sigma_i{=}(S_i^1, S_i^2)$ as

$$\begin{cases} S_i^1{=}R_i{+}h(M_i||ID_i)CSK_i \\ S_i^2{=}x_iP \end{cases} \tag{9}$$

where x_i is the horizontal coordinate of the point R_i. Then V_i sends the message packet <ID_i, M_i, σ_i, T_i> to the DRA via *AMB*. *AMBs* can just forward vehicles' messages to the DRA in this kind of communication, but could not verify the messages, because the secret key k_i is only known to the vehicle and the DRA. In order to achieve the communication between vehicles, a group communication scheme is described in the next section.

The vehicle's message can be verified one by one or in batch by DRA. Batch verification can achieve verifying a number of messages at once, to save computational overhead and verification time. The batch verification can also make the DRA react timely to the disaster situation and dispatch the nearby ambulance. Next, the processes of batch verification are introduced in detail.

Given n distinct signatures σ_1, σ_2, σ_3, …, σ_n received from V_1, V_2, V_3, ……, V_n respectively, the DRA first checks the timestamp in the message, verifies the freshness of the message, and deletes outdated ones. Then DRA calculates the vehicle's private key and the point R_i with k_i. Until now, it's the same as single message authentication. Finally, DRA verifies all the signatures in one operation. The specific verification steps are as follows:

- For freshness, DRA first checks the transmission delay. Assuming the time DRA receiving the message is T_n, DRA checks whether $\Delta T \geq T_n - T_i$ is valid, where ΔT is the preset maximum transmission delay. If the inequality holds, then continue the verification; otherwise, the DRA discards the outdated message. This step is done for every message.
- DRA calculates the vehicle's corresponding private key according to (8) $CSK_i{=}h(ID_i||k_i)P$.
- Calculate the point $R_i{=}S_i^1\text{-}h(M_i||ID_i)CSK_i$.
- Authenticate all the signatures by verifying if (9) holds: $S_i^2 \overset{?}{=} \sum_{i=1}^{n}(x_i)P$.

The DRA needs to find out the shared secret k with V_1, V_2, V_3, …, V_n respectively, by checking which of the stored pairs (RID_i, k_i) satisfy (7) $ID_i^2{=}RID_i \oplus H(k_i||ID_i^1 \,||\, LT_i)$. During the verifying process, the private key CSK_i and the random point R_i need to be calculated to achieve authentication. However, the security of our scheme is not destroyed. The DRA is completely trustable, and the private key can not reveal the vehicle's real identity. In addition, vehicles change the pseudonym periodically.

2. Scheme2: vehicle group communication

The above verification processes are only suitable for communication between the vehicle and the DRA. During the rescue process, vehicles also need to communicate with each other to timely exchange information. Therefore, we designed a vehicle group communication scheme, which is based on the aforementioned pseudonym signature. Signing and verification only require point multiplications to ensure fast verification and reduce the computational overhead.

1) Group formation

This sub-section shows how a group of known vehicles form a communication group, and how they securely communicate with each other. The establishment of the group is divided into four stages: application stage, agreed stage, validation stage, and key establishment stage.

- *AMB* launches the message M_i={GR, ID_1, ID_2, ID_3, …, ID_n} to start the group establishment, where GR indicates it's the group request message.
- Vehicle receiving the message checks for its own pseudonym ID_j. If found, it signs the agreed message M_j={GA, ID_j} and sends it to DRA via *AMB*.

- Receiving the request message and all the agreed messages, the DRA batch-verifies all the signatures. Only if the verification succeeds, the DRA carries on to the group key generation phase. Otherwise, the DRA suspends the protocol and waits for new request.
- If all the signatures are valid, the DRA establishes the group key for the group members. It selects a random number *ran*, and sets the group private key as $GSK=s\times ranP$, while the group public key for each member is set $GPK_i=k_iP$. The DRA encrypts the shared group private key with each k_i respectively, and broadcasts the message $M=\{ID_1, ID_2, \ldots, ID_n, E_{k_1}(GSK), E_{k_2}(GSK), \ldots, E_{k_n}(GSK)\}$ with its signature $SIG_{SK_{DRA}}(M)$. The group members first verify DRA's signature and then conduct decryption with the k_i to get the group private key *GSK*.

2) Group communication

Vehicles can authenticate each other within the group to realize real-time communication. Note that DRA is still able to verify the group messages. With the pre-generated pseudonym (7), and the group private key *GSK*, a vehicle generates the group message signature σ_i as

$$\begin{cases} S_i^1 = R_i + h(M_i \| ID_i)GSK \\ S_i^2 = x_iP \end{cases} \tag{10}$$

The *GSK* is employed to generate signatures of group message. The group message is broadcasted in the format $<ID_i, M_i, \sigma_i, T_i>$, where two bits can be added to distinguish the group message and vehicle-to-DRA message. But these two bits are not counted in the communication overhead.

Receiving the message, the verifier V_j first checks the time validity. If the aforementioned step is valid, it comes to the signature verification. Firstly, V_j calculates the point $R_i=S_i^1-h(M_i)GSK$ with the group private key *GSK*. Then, V_j verifies the signature by checking whether $S_i^2 = x_iP$ holds. Note that batch verification is also applicable to the group communication, providing a much smaller computing overhead and verification delay. Vehicles and the DRA can both carry out batch verification to achieve efficiency. In Scheme1, $(2n+1)$ point multiplications are needed when the DRA verifies n message, while in Scheme2, only $(n+1)$ point multiplications.

D. Discussion

Traceability: Given the pseudonym ID_i, only the trust authority DRA, having the shared secret k_i, can trace the actual identity RID_i. Therefore, once vehicles are in dispute about a signature or are found to abuse the VANETs, the DRA has the ability to trace the vehicle from the disputed message signature, by which the traceability can be well satisfied. The tracking process is as follows:

$$\begin{cases} ID_i^2 \oplus H(k_i \| ID_i^1 \| LT_i) = RID_i \\ RID_i \oplus H(k_i \| ID_i^1 \| LT_i) \oplus H(k_i \| ID_i^1 \| LT_i) = RID_i \end{cases} \tag{11}$$

Invalid signature detection: If there is one invalid signature in the batch, it will lead to failure of the entire batch verification. In VANETs, invalid signature may be caused by many cases, like malicious vehicles or the hardware malfunction of legitimate vehicles. Therefore, invalid signature detection mechanism is necessary. We adopt the binary search method to check for invalid signatures, as ABAKA [14]. When the batch verification fails, the batch is bisected, and verified respectively until only one message left or valid.

Revocation check: Before joining the network, new vehicles need to complete registration with the DRA via *AMB*. When DRA receives V_i's request, it must check if the requesting vehicle is in the sorted revocation list (RL) by running Algorithm 1. If the returned value of Algorithm 1 is 1, the revocation is detected. Then DRA rejects the registration request. Otherwise, DRA continues the registration process.

Algorithm 1 *Revocation Detection*

```
RDetAlg(RL, $l$, $r$, $RID_i$):
begin
$mid=\lfloor \frac{l+r}{2} \rfloor$;
if RL[$mid$]=$RID_i$ then
    return Found=1;
else if RL[$mid$]>$RID_i$ then
    $r=mid-1$;
    RDetAlg(RL, $l$, $r$, $RID_i$)
else
    $l=mid+1$;
    RDetAlg(RL, $l$, $r$, $RID_i$);
end if
end
```

V. Security Analysis

We analyze of the security performance of the proposed scheme in this chapter. According to the security objectives aforementioned, we mainly focus on the following four aspects: sender authentication and message integrity, internal attacks prevention, conditional privacy protection and revocability, efficiency.

1) Sender authentication and message integrity: The proposed scheme EPAS securely achieves session key establishment, mutual authentication between vehicles, and DRA batch-verifying vehicles messages. The adopted Diffie-Hellman session key agreement scheme secured with signature has been proven secure. The vehicle generates pseudonym and corresponding private key with the unique secret key, which guarantees no one else can forge its pseudonym and signature. Once the message content is distorted during the transportation, the signature verification can't be valid. This ensures that only the unmodified messages from legitimate senders are accepted.

2) Internal attacks prevention: An important security property of our EPAS is the ability to prevent internal attacks. Even if an attacker has captured some legitimate vehicles and their private secrets, the attacker still can't use the information to forge other legitimate vehicle's signature. In addition, the damage caused by the captured

vehicles is also limited, because the tracking mechanism can quickly determine the real identity of these vehicles, and TA can promptly revoke the malicious vehicles from the network.

3) Conditional privacy protection and revocability: The actual identity of a vehicle is concealed by the pseudonym. On the other hand, the authority DRA, and only the DRA can reveal the real identity. For example, once V_i is found misbehaving, the ID_i is reported to DRA. The DRA traces the real identity RID_i through (11) and sends it to TA, who determines whether to revoke V_i or not. The specific revocation mechanism is out of the scope of our paper.

4) Efficiency: Pseudonym mechanism is adopted in order to save communication overhead. To achieve fast authentication and save the computational overhead, we employ the idea of batch validation. In addition, the signature is generated through point multiplications, whose computational overhead is just 0.6ms much smaller than 4.5ms of bilinear pairing. The message verification procedure only needs two point multiplications in the group communication scheme, which can significantly improve the efficiency.

VI. Performance Evaluation

In this section, we evaluate the performance of the proposed scheme EPAS in terms of verification delay and transmission overhead. In the simulation, our scheme EPAS is compared with three related typical schemes IBV [13], ABAKA [14], and ECDSA [23]. IBV and ABAKA are typical batch verification schemes, while ECDSA signature scheme is adopted by the current standard IEEE 1609.2 and some other schemes such as RAISE [11].

A. Verification Delay

Let T_{mtp} denotes the time of a MapToPoint hash operation, T_{mul} the time of performing one point multiplication over an elliptic curve, and T_{par} the time of a bilinear pairing operation. According to [24], T_{mul} is 0.6 ms, T_{mtp} is 0.6 ms and T_{par} is 4.5ms. So the operation time of T_{mul} and T_{mtp} is much smaller than T_{par}. The computation cost mainly focus on the above three parameters. Our EPAS doesn't need the pairing operation. We don't consider the cost of one-way hash function, which is only 2 microseconds. The computational overhead of the schemes is given in Table III.

TABLE III.
COMPUTATIONAL OVERHEAD

Schemes	Authenticate a single message	Authenticate n messages
IBV	$3T_{par}+T_{mtp}+T_{mul}$	$3T_{par}+nT_{mtp}+nT_{mul}$
ECDSA	$4T_{mul}$	$4nT_{mul}$
ABAKA	$7T_{mul}$	$(2n+5)T_{mul}$
EPAS: Scheme1	$3T_{mul}$	$(2n+1)T_{mul}$
EPAS: Scheme2	$2T_{mul}$	$(n+1)T_{mul}$

From the comparison, we can see the proposed scheme EPAS Scheme2 achieves the least verification overhead for both one-by-one message authentication and batch verification. To verify n distinct signatures, IBV needs $3T_{par}+nT_{mtp}+nT_{mul}$, ECDSA $4nT_{mul}$ and ABAKA $(2n+5)T_{mul}$, while our scheme EPAS only $(2n+1)T_{mul}$ and $(n+1)T_{mul}$. The ECDSA verifies n distinct signatures one by one, so the n-messages verification is not efficient. In addition, since ECDSA is not identity based, additional operations are needed to verify the certificate of public key. Although IBV is a batch verification scheme, the basic pairing operation is computational costly. The verification cost of ABAKA is close to that of our Scheme1, but much higher than the Scheme2.

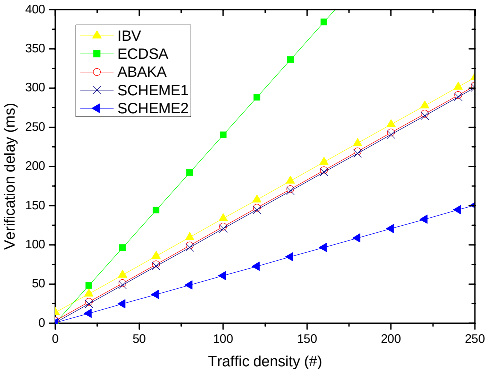
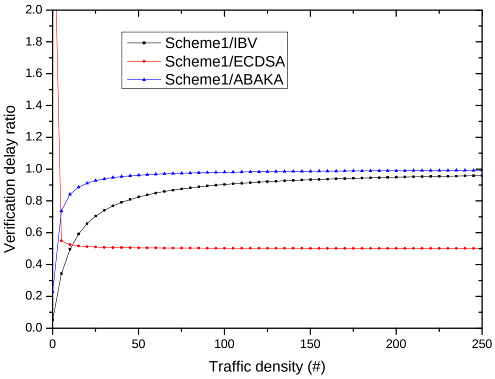


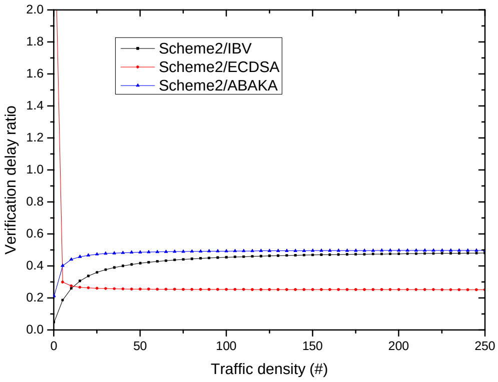
Figure 3. Verification delay with different traffic density

The verification delay of all the five schemes is obviously presented in Fig. 3. We can see from the figure apparently that the computational overhead and the verification delay increase linearly with the number of messages for all these schemes. Our EPAS is superior to all the other typical schemes, especially Scheme2. This is because our EPAS adopts lightweight point multiplications to sign and verify messages.

The ratio of the message verification delay of these schemes is shown in Fig. 4, with (a) for Scheme1 and (b) for Scheme2 respectively. It is obvious that the delay ratio between EPAS Scheme2 and IBV is always less than 0.50 no matter the number of messages; the delay ratio between EPAS Scheme2 and ECDSA is approximately 0.25 when the number of messages is larger than 60. In other words, the verification speed of EPAS is twice of IBV's, and is almost 70% faster than the current standard ECDSA.



(a)



(b)

Figure 4. Verification delay ratio with different traffic density

B. Transmission Overhead

In this sub-section, we compare the transmission overhead of the five schemes. The comparison is in terms of the signature and the certificate appended to the original message, while the message itself is not counted.

As shown in Table Ⅳ, for IBV, the length of signature is 21 bytes, and 42 bytes for pseudonym. ABAKA's authentication materials consist of 20 bytes verification message and 20 bytes material message, resulting in a signature of 40 bytes. ECDSA signature is 42 bytes, but a certificate of 125 bytes must be transmitted along with the message. And the total transmission overhead of the ECDSA scheme is 167 bytes. Besides, as the number of messages increases, the transmission overhead increases linearly for all the schemes.

TABLE IV.
TRANSMISSION OVERHEAD

Schemes	One message	*n* messages
IBV	63B	63*n*B
ECDSA	167B	167*n*B
ABAKA	80B	80*n*B
EPAS: Scheme1	82B	82*n*B
EPAS: Scheme2	82B	82*n*B

Since the IBV scheme adopts bilinear pairing cryptographic operations for signature, which is short in length but costly in verification, the total transmission overhead of IBV is 63 bytes as the shortest. The transmission overhead of ECDSA is the largest because of certificate overhead. Our two proposals have the same transmission cost, which is a bit larger than ABAKA as 2 bytes life period LT_i is added to the pseudonym in our scheme to prevent expired pseudonyms abuse. Although the transmission overhead of IBV is much smaller than the other four schemes, it has a serious flaw of signature forging, which makes IBV inapplicable to safety applications.

VII. Conclusion

In this paper, we have proposed an Efficient Privacy-preserving Authentication Scheme (EPAS) for VANETs-based emergency communication, which contains two efficient communication patterns: vehicle-to-DRA communication and vehicle group communication. The EPAS adopts pseudonym based signature, effectively preventing the leak and track of vehicle's privacy information. On the other hand, the authority can trace the malicious vehicle to protect the security of VANETs. From the experiment results, the proposed scheme relieves the bottleneck problem of one-by-one message verification, and reduces the computational overhead and the transmission overhead in VANETs. But the performance analyses of the proposed scheme are not very comprehensive and we have not explored the specific revocation mechanism.

References

[1] Dedicated Short Range Communications (DSRC), Available: http://www.etsi.org/index.php/technologies-clusters/technologies/intelligent-transport/d src.

[2] USA Department of Transportation, "National Highway Traffic Safety Administration", Vehicle Safety Communications Project, Final Repot, 2006.

[3] S Lee, G Pan, J Park, M Gerla, S Lu, "Secure incentives for commercial ad dissemination in vehicular networks", In Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'07), pp.150-159, 2007.

[4] A Studer, E Shi, F Bai, and A Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs", In Proceedings of the IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), pp.22-26, June 2009.

[5] R Chen, D Ma, A Regan, "TARI: Meeting Delay Requirements in VANETs with Efficient Authentication and Revocation", In Proceedings of WAVE, 2009.

[6] D Boneh, H Shacham, "Group signatures with verifier-local revocation", In Proceedings of the ACM conference on Computer and communications security(CCS), pp.168-177, 2004.

[7] B-K Chaurasua, S Verma, "Conditional privacy through ring signature in vehicular ad-hoc networks", Transactions on Computational Science, Springer, vol. 6750, pp.147-156, 2011.

[8] R-X Lu, X-D Lin, T-H Luan, "Pseudonym changing at social spots: an effective strategy for location privacy in VANET", IEEE Transaction on Vehicular Technology, vol. 61, no. 1, pp.86-96, Jan, 2012,.

[9] M Raya, J-P Hubaux, "Securing vehicular ad hoc networks", Computer Security, IOS, vol. 15, no. 1, pp. 39-68, Jan. 2007.

[10] X Lin, X Sun, P-H Ho, X Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications", IEEE Transactions on Vehicular Technology. vol. 56, no. 6, pp. 3442-3456, Nov. 2007.

[11] C Zhang, X Lin, R Lu, P-H Ho, X. Shen, "An efficient message authentication scheme for vehicular communications", IEEE Transaction Vehicular Technology, vol. 57, no. 6, pp. 3357-3368, Nov. 2008.

[12] Y Hao, Y Cheng, CH Zhou, W Song, "A Distributed Key Management Framework with Cooperative Message Authentication in VANETs", IEEE Journal on selected areas in communications, vol. 29, no. 3, pp.616-629, Mar. 2011.

[13] C Zhang, R Lu, X Lin, P-H Ho, X. Shen, “An Efficient Identity-based Bath Verification Scheme for Vehicular Sensor Networks”, INFOCOM, pp.246-250, 2008.

[14] J-L Huang, L-Y Yeh, H-Y Chien, “ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular”, IEEE Transaction On Vehicular Technology, vol. 60, no. 1, pp. 248-262, Jan. 2011.

[15] K-A Shim, “CPAS: An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks”. IEEE Transactions on Vehicular Technology, vol.61, no.4, pp.1874-1883, May 2012.

[16] 2008 Sichuan Earthquake. Available: http://en.wikipedia.org/wiki/2008_Sichuan_earthquake.

[17] X Guo, T Feng, ZH Yuan, “Multiple Node-disjoint Paths Distance Vector Routing for Ad hoc Networks”, Computer Science, vol. 38, no. 2, pp. 86-91,2011.

[18] C Ren, “Solving Min-Max Vehicle Routing Problem”, Journal of Software, vol. 6, No. 9, pp. 1851-1856, Sep. 2011. doi:10.4304/jsw.6.9.1851-1856

[19] J Li, “Vehicle Routing Problem with Time Windows for Reducing Fuel Consumption”, Journal of Computers, vol. 7, No. 12, pp. 3020-3027, Dec. 2012. doi:10.4304/jcp.7.12.3020-3027

[20] D Hankerson, A Menezes, S Vanstone, “Guide to Elliptic Curve Cryptography”, Springer-Verlag, 2004.

[21] F Li, X Xin, Y Hu, “Identity-based broadcast signcryption”, Computer Standard & Interfaces, vol. 30, no. 1-2, pp. 89-94, Jan. 2008.

[22] J-H Yang, C Chang, “An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem”, Computer Security, vol. 28, no. 3-4, pp. 138-143, 2009.

[23] IEEE Standard 1609.2 - IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, July 2006.

[24] C Zhang, P-H Ho and J Tapolcai, “On batch verification with group testing for vehicular communications” ,Wireless Networks, vol.17, no. 8, pp. 1851-1865, 2011.

Xuedan Jia was born in China in 1988. She is a master degree candidate in Jiangsu University. Her research interests include secure authentication and privacy preservation technology for VANETs.

Liangmin Wang was born in China in 1977. He is an associate professor in Jiangsu University and a special term professor in Anhui University. His research interests include security and privacy-preserving technology for the Internet of Things.